一个改进的强指定验证者签密方案 *

李元晓 [1,2]，周彦伟 [1,2]，杨　波 [1,2†]

(1. 陕西师范大学 计算机科学学院，西安 710119；2. 中国科学院信息工程研究所，信息安全国家重点实验室，北京 100093)

摘　要：Sujata 等人在 2012 年提出了一个基于离散对数的强指定验证者签密方案，然而分析可知 Sujata 等人的方案无法抵抗授权攻击，并且验证权具有可委托性。针对上述不足，给出一个改进的强指定验证者签密方案，仅有指定的验证者才能验证签密密文的有效性；此外，指定的验证者能够生成一个与原始签密密文不可区分的签密副本。安全分析表明，该方案不仅能够抵抗适应性选择明文攻击，而且在提供认证的同时可保证签密密文的不可伪造性。由于该方案的上述优越性能，在实际生活中具有广泛的应用前景，如区块链、电子投票、电子招标等场景。

关键词：强指定验证者签密；授权攻击；不可伪造；不可区分

中图分类号：TP309.7　　doi: 10.19734/j.issn.1001-3695.2018.07.0558

Improved strong designated verifier signcryption scheme

Li Yuanxiao[1, 2], Zhou Yanwei[1, 2], Yang Bo[1, 2†]

(1. *School of Computer Science*, *Shaanxi Normal University*, *Xi'an* 710119, *China*; 2. *State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*)

Abstract: In 2012, Sujata et al. proposed a strong designated verifier signcryption scheme based on discrete logarithm. However, it cannot resist the delegable attack. In this paper, this paper proposed a strong designated verifier signcryption scheme, in which, the designated verifier can only verify the validity of the message. At the same time, the designated verifier can generate a signed transcript that is indistinguishable with the original signed ciphertext. Through the security analysis, proposed scheme can resist the adaptive choice plaintext attacks. In addition, it can guarantee the non-forgery of the signed ciphertext while providing authentication. Due to the above superior performance of the scheme, proposed solution can be applied to blockchain, electronic voting, tendering, and other realistic scenarios.

Key words: strong designated verifier; delegable attack; unforgeable; indistinguishable

0　引言

签密是 1997 年由 Zheng[1]首次提出的一种新的密码学原语，签密能够在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能，而其计算量和通信成本都要低于传统的“先签名后加密”。在签密方案中，签密文本发送者通常用接收者的公钥生成一个实现两者之间对称加密的会话密钥，接收者用自己的私钥也可以产生一个相同的会话密钥，此会话密钥安全性是认证和加密的安全保障。

为增强签名者的隐私性，Jakobsson 等人[2]首次提出强指定验证者签名（strong designated verifier signature,SDVS）的概念。只有指定验证者相信签名的有效性。然而，任何得到签名的人可以验证签名有效性，即可判断真正签名者是两者中的一个。为了解决这个问题，2003 年 Saeednia 等人[3]提出了一个强指定验证者签名方案，这个方案中只有拥有指定验证者私钥的人才可以验证签名的有效性。与此同时，Saeednia 等人[3]首次提出强指定验证者签密的概念，强指定验证者签密将签密和指定验证者结合起来，在实现可否认认证的同时，保证消息机密性。

2005 年 Lipmaa 等人[4]提出一个针对指定验证者签名的攻击模型，命名为授权攻击。因此为指定验证者签名增加了一个新的安全属性（称之为非授权性），并证明已有几个指定验证者签名方案都不能抵抗授权攻击。授权攻击的基本思想是，签名者或者指定验证者可以在不泄露自身私钥的情况下，把签名权或者验证权授权给第三方，这是安全的指定验证者签名方案不希望具备的性质。

2012 年，Sujata 等人[5]提出了一个基于离散对数的强指定验证者签密方案，然而分析可知 Sujata 等人的方案无法抵抗授权攻击，并且验证权具有可委托性，为此本文给出一个改进的强指定验证者签密方案。在此方案中签密文本只能被指定验证者验证，在实现相同功能的条件下计算效率远远高于文献[6,7]方案，并给出了安全性和效率分析。

1　数学基础

1.1　离散对数问题

设 p 是素数，a 是 p 的本原根，即 $a^1, a^2, \ldots, a^{p-1}$ 在模 p 下产生 1 到 $p-1$ 的所有值，所以对 $\forall b \in \{1, 2, \ldots, p-1\}$，有唯一的 $i \in \{1, 2, \ldots, p-1\}$ 使得 $b = a^i \bmod p$，称 i 为模 p 下以 a 为底 b 的离

收稿日期：2018-07-11；**修回日期：**2018-08-28　**基金项目：**国家重点研发计划资助项目（2017YFB0802000）；国家自然科学基金资助项目（61572303, 61772326, 61802241, 61802242）；国家“十三五”密码发展基金资助项目（MMJJ20180217）；中国科学院信息工程研究所信息安全国家重点实验室开放课题（2017-MS-03）

作者简介：李元晓（1992-），女，山西运城人，硕士研究生，主要研究方向为公钥密码学（liyuaanxiao@163.com）；周彦伟（1986-），男，甘肃定西人，工程师，博士，主要研究方向为密码学、匿名通信技术；杨波（1963-），男（通信作者），陕西富平人，教授，博士，主要研究方向为公钥密码学等.

散对数，记为 $i \equiv \log_a b \bmod p$ 。当 a 、 p 、 i 已知时，用快速指数算法可比较容易地求出 b ，但当 a 、 b 和 p 已知时，求 i 则非常困难。目前已知的最快的求离散对数算法其时间复杂度为 $O(\exp(\ln p)^{1/3}\ln(\ln)^{2/3})$ ，所以当 p 很大时，该算法也是不可行。

1.2　安全模型

1.2.1 不可区分性

如果对任何多项式时间敌手 A ，存在一个可忽略的函数 $\varepsilon(k)$ ， k 为安全参数，使得 $Adv_{\Pi,A}^{CPA}(k) \le \varepsilon(k)$ ，那么就称这个算法 Π 是语义安全的，或者称为在选择明文攻击下具有不可区分性，简称为 IND-CPA 安全。如图 1 所示，具体游戏描述如下[14]：

a)挑战者运行密钥生成算法生成签密文本接收者的公私钥对 (sk_b, pk_b) ，并将 pk_b 发送给敌手 A 。

b)敌手在进行签密询问时，选择一个消息 $m \in M$ 和接收者的公钥 pk_b 将其发送给挑战者。挑战者模拟签密预言机，对 (m, sk_a, pk_b) 进行签密，然后返回相应的结果给敌手 A 。

c)敌手 A 选择两个相同长度的消息 $m_0, m_1 \in M$ 和一个公钥 pk_b 发送给挑战者，挑战者随机选择 $r \in \{0,1\}$ ，计算一个对于消息 m_r 、签密者的私钥 sk_a^* 、指定验证者的公钥 pk_b^* 的签密文本 $\delta' = Signcryption(m_r, sk_a^*, pk_b^*)$ ，并将 δ' 发送给敌手 A 作为挑战密文。

d)敌手输出 r' 。如果 $r = r'$ 则敌手区分成功。敌手 A 的优势可定义为参数为 k 的函数： $Adv_{\Pi,A}^{CPA}(k) = |\Pr[r' = r] - 1/2|$ 。

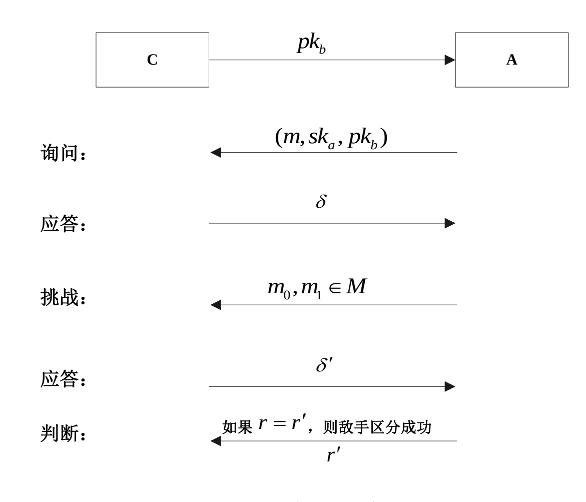


图 1　不可区分性游戏过程图

Fig. 1　The process of indistinguishable game

1.2.2 不可伪造性

如果对任何多项式时间敌手 A ，存在一个可忽略的函数 negl ，使其满足 $\Pr[\text{Sig-forge}_{A,\Pi}(n) = 1] \le \mathrm{negl}(n)$ ，那么就称这个签名方案 $\Pi = (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Vrfy})$ 在适应性选择消息攻击下是存在性不可伪造的，简称为 EF-CMA 安全。如图 2 所示，具体游戏描述如下[15]：

a)挑战者运行密钥生成算法，生成签密文本接收者的公私钥对 (sk_b, pk_b) ，并将 pk_b 发送给敌手 A 。

b)敌手在进行签密询问时，选择一个消息 $m \in M$ 和接受者的公钥 pk_b 将其发送给挑战者。挑战者模拟签名预言机，对 (m, sk_a, pk_b) 进行签名，并将结果返回给敌手 A 。

c)敌手 A 选择一个相同长度的消息 $m' \in M$ 和公钥 pk_b 发送给挑战者，计算一个对于消息 m' 、签密者的私钥 sk_a 、指定验证者的公钥 pk_b 的签密文本 δ' ，并将 δ' 发送给敌手 A 作为挑战密文。

d)敌手输出 (m', δ') 。如果 $\mathrm{Vrfy}_{pk_b}(m', \delta') = 1$ 且 m' 之前没有询问过，则敌手伪造成功。

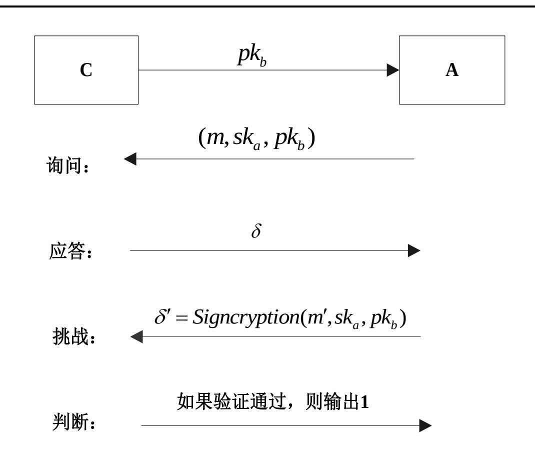


图 2　不可伪造性游戏过程图

Fig. 2　The process of unforgeable game

2　Sujata 强指定验证者签密方案

2.1　方案概述

该方案首先生成用户的公开参数：两个安全素数 p, q（ q 为 $p-1$ 的素因子），生成元 $g \in Z_p$ 阶为 q ，单向哈希函数 H ，输出的值属于 Z_p 。签名者 Alice 拥有自己的密钥对 (x_a, y_a) 。Alice 选择自己的私钥 $x_a \in Z_q$ ，计算相对应的公钥 $y_a = g^{x_a} \bmod p$ ，同样，指定验证者 Bob 也有自己的密钥对 (x_b, y_b) 其中 $y_b = g^{x_b} \bmod p$ 。

1）签密的生成

a）Alice 随机选择 $t \in Z_q$ ；

b）Alice 计算 K, r, s, C 如下：

$$K = y_b{}^t \bmod p$$

$$C = E_K(m)$$

$$r = H(K)$$

$$s = t - rx_a \bmod q$$

c）Alice 发送签密文本 $\delta = (r, s, C)$ 给指定接收者 Bob；

2）解签密

a）Bob 收到签密文本 $\delta = (r, s, C)$ 后，用私钥 x_b 计算出 K' ：

$$K' = (g^s y_a{}^r)^{x_b} \bmod p$$

b）验证 $r = H(K')$ ；

c）计算 $m = D_{K'}(C)$ 。

2.2　方案分析

指定验证者签名的本意是指：Alice 向 Bob 证明论断 Θ 的正确性，通过证明“ Θ 是正确的”或“她知道 Bob 的私钥”来实现。但是此指定验证者签名方案设计时，变换成证明命题“ Θ 是正确的”或“她知道部分信息”，这个部分信息是关于 Alice 私钥（公钥）和 Bob 公钥（私钥）的单向函数，即已知这个单向函数是无法得到私钥的。在密码学中，除了私钥被严格保护之外，其他任何组成在各种各样的攻击下都是脆弱的，都有被攻破的可能性。

此方案具有可授权性的缺陷，具体描述如下：

给定 $y_{ab} = g^{x_a x_b} \bmod p$ 的知识[8]，任何人在没有指定验证者私钥的情况下都可以验证 $r = H(y_b{}^s y_{ab}{}^r \bmod p) = H(K)$ 是否成立。因为任意第三方在得到 $\delta = (r, s, C)$ 后，计算 $K = y_b{}^s y_{ab}{}^r \bmod p = (g^s y_a)^{x_b r} \bmod p$ ，即可在不知道指定验证者 Bob 的私钥的情况下，验证 $r = H(y_b{}^s y_{ab}{}^r \bmod p)$ 是否成立，因此违背了强指定验证者的定义。攻击者在消息未到达指定验证者之前提取出 $y_{ab} = g^{x_a x_b} \bmod p$ 的知识，解签密后一方面可对密文进行解密，另一方面可得知签密的真实来源，这对于强指定验证者签密来说是极不安全的。

3 本文方案的构造

本文给出了一个新的强指定验证者签名的签密方案，此方案可抵抗授权攻击，相对于 Sujata 的签密方案有一定的安全性提升。本方案基于 Lee 的强指定验证者签名方案[9]，将 Schnorr 签名[10]和 Wang 的可认证加密方案[11]结合，本文的方案使用安全的对称加密算法 $(E_K(\cdot), D_K(\cdot))$ 。

a)系统初始化:两个安全素数 p, q （q 为 $p-1$ 的素因子），生成元 $g \in Z_p$ 阶为 q，单向哈希函数 H，输出的值属于 Z_p 。

b)密钥生成:Alice 选择自己的私钥 $x_a \in Z_q$，计算相对应的公钥 $y_a = g^{x_a} \bmod p$，同样，指定验证者 Bob 也有密钥对 (x_b, y_b) 其中 $y_b = g^{x_b} \bmod p$ 。

c)签密的生成

(a)Alice 选择一个随机值 $k \in Z_q$；

(b)Alice 以如下方式计算 r, s 和 t：

$$r = g^k \bmod p$$

$$s = k + x_a r \bmod q$$

$$c = {y_b}^s \bmod p$$

(c)Alice 将 c 按位平均截成左右两半部分 c_1, c_2 （若 c 长度为奇数，则左短右长），并计算：

$$t = H(m, c_1)$$

$$D = Enc_{c_2}(m)$$

(d)Alice 生成的签密文本为 $\delta = (r, t, D)$ 。

d）解签密

(a)Bob 收到签密文本 $\delta = (r, t, D)$ 后，用自己的私钥 x_b 计算出 c'：

$$c' = (r{y_a}^r)^{x_b} \bmod p$$

(b)Bob 以相同的方式将 c 分成两部分，计算：

$$m = Dec_{c_2'}(D)$$

$$t = H(m, c_1')$$

(c)如果 (b) 中等式成立则签密文本验证通过。

e）签密副本的生成

指定验证者签名的特性是只有被事先指定的验证者才能知道签名的真实来源，验证者无法让任意第三方相信签名的真实来源。任意第三方之所以不能知道签名的真实来源，是因为指定验证者也可以生成一个与签名者签名不可区分的签名副本。为了使第三方难以区分出传送的签密文本是 Alice 生成的还是 Bob 生成的，Bob 验证通过后模拟生成签密副本 δ'，具体过程如下：

(a)Bob 选择一个随机值 $k' \in Z_q$；

(b)Bob 以如下方式计算出 r', t', D'：

$$r' = g^{k'} \bmod p$$

$$c' = (r'{y_a}^{r'})^{x_b} \bmod p$$

(c)以相同的方法将 c' 分成两部分 c_1', c_2' ,计算：

$$t' = H(m, c_1')$$

$$D' = Enc_{c_2'}(m)$$

(d)Bob 生成的签密副本为 $\delta' = (r', t', D')$ 。

4 方案的安全性与效率分析

由于方案中 $c = (r{y_a}^r)^{x_b} \bmod p$，仅掌握签密者和指定验证者的公钥以及 y_{ab} 的知识是不能够生成一个有效的签名以及验证签名的有效性，因为即使掌握了这些知识生成一个有效签名或者验证签名有效性，面对的问题仍然是求解离散对数问题。本文的方案具有不可伪造性、机密性、不可传递性以及不可授权性。

4.1 正确性

接收者 Bob 收到签密文本 $\delta = (r, t, D)$ 后可正确验证签名的有效性，原因如下：

a) $c' = (r{y_a}^r)^{x_b} = g^{(k + x_a r)x_b} = {y_b}^{k + x_a r} = {y_b}^s = c$ 将 c' 同样的方法分成两部分 c_1', c_2'；

b)当 $c_2' = c_2$ 时， $m = Dec_{c_2'}(D) = Dec_{c_2}(D)$；

c)当 $c_1' = c_1$ 时 ， $t = H(m, c_1) = H(m, c_1')$ 。

4.2 机密性

除了指定接收者，其他任何人不能从签密文本中提取出任何关于消息 m 的任何信息。

因为哈希函数的单向性，在恢复 $c' = (r'{y_a}^{r'})^{x_b} \bmod p$ 后，很难从 $t = H(m, c_1)$ 得到关于消息 m 的任何信息。

因为 $(Enc_k(\cdot), Dec(\cdot))$ 为安全的对称加密解密算法对。必须得到密钥才能进行解密，要想得到密钥，必须知道 k 和 x_a，又因为离散对数问题的困难性，所以很难从 $r = g^k \bmod p$ 和 $y_a = g^{x_a} \bmod p$ 中得到 k 和 x_a，因此本方案是安全的。

引理 1 对于所有的概率多项式时间敌手 A，存在一个可忽略的函数 $negl$，满足 $\Pr[\mathrm{PrivK}_{A,\Pi}^{cpa}(n) = 1] \le \frac{1}{2} + negl(n)$，则敌手 A 在选择明文攻击下是不可区分的。

在方案中如果敌手 A 成功区分出 m_0, m_1，即 $r = r'$，则意味着敌手攻破了安全的对称加密方案。因为对称加密的密文不可区分性，所以本文的方案是不可区分的。这里的对称加密可以用别的方式构造，且可证明安全，这里为了方案的工整性，不做详细描述。

4.3 不可伪造性

方案使用 Schnorr 签名生成 (r, s)，根据[4]中 Schnorr 签名的可证明安全性，任何适应性敌手，包括 Bob 不能伪造一个对消息 m 的签密文本 $\delta = (r, t, D)$，满足： $m = Dec_{c_2}(D)$， $t = H(m, c_1)$ 其中 $r = g^k \bmod p$， $s = k + x_a r \bmod q$ $c = {y_b}^s \bmod p$ 。否则敌手可以成功伪造一个合法的 Schnorr 签名。所以本方案是安全的。

引理 2 如果不存在任何概率多项式时间算法能以不可忽略的概率赢得以上游戏，则称方案在适应性选择消息攻击下是存在性不可伪造的。

如果上述游戏中，敌手对挑战者进行一系列的询问之后，向挑战者返回一个合法的消息签密文本，那么将敌手伪造签密的能力规约到敌手攻破 schnorr 签名的问题上。因为 schnorr 签名是不可伪造的，所以本文的方案是不可伪造的。

4.4 不可授权性

本方案中 $t = H(m, (r{y_a}^r)^{x_b} \bmod p) = H(m, {y_b}^k {y_{ab}}^r)$,仅掌握签密者和指定验证者的公钥以及 y_{ab} 的知识是不能够生成一个有效的签名以及验证签名的有效性，该方案在验证过程中不存在可授权性的缺陷，只有掌握了指定验证者私钥的人才能验证签名的有效性，面临的问题是离散对数问题，这在现有的计算能力下是困难问题。

4.5 不可转移性

Bob 生成的签密副本 $\delta' = (r', t', D')$ 与 Alice 的签密 $\delta = (r, t, D)$ 是不可区分的，从 Alice 的有效签密文本里随机选的一个 $(\bar{r}, \bar{t}, \bar{D})$，因为 (r, t) 都是由 $k \in Z_{q^*}$ 决定，(r', t') 由 $k' \in Z_{q^*}$ 决定， D' 和 D 是不可区分的，所以

$$\Pr[(\mathrm{r}, \mathrm{t}, \mathrm{D}) = (\bar{r}, \bar{t}, \bar{D})] = \frac{1}{q-1}$$

$$\Pr[(r', t', D') = (\bar{r}, \bar{t}, \bar{D})] = \frac{1}{q-1}$$

因此 Bob 生成的签密副本 $\delta'=(r',t',D')$ 与 Alice 的签密 $\delta=(r,t,D)$ 的分布是相同的，因此是不可区分的。

4.6 效率分析

在本方案中，签密阶段的计算复杂度为 $2T_E+1T_H+1T_M$，解签密文本的过程中的计算复杂度为 $2T_E+1T_H+1T_M$。（T_E,T_H,T_M,T_B 分别代表模指数运算、哈希运算、模乘运算、双线性映射运算）。与文献[2]相比，实现可抵抗授权攻击的性质的同时不增加额外的开销。此外，本文分析等功能的签密方案计算效率，性能比较结果如表 1 所示。

表 1 相关方案的性能比较结果表

Table 1 The performance of the relevant scheme

相关方案	签密	解签密	总计算开销
文献[6]	$3T_E+3T_B+T_M+2T_H$	$4T_E+4T_B+3T_H$	$7T_E+7T_B+T_M+5T_H$
文献[7]	$4T_E+4T_B+T_M+3T_H$	$4T_E+4T_B+4T_H$	$8T_E+8T_B+T_M+7T_H$
文献[2]	$1T_E+1T_H+1T_M$	$3T_E+1T_H+1T_M$	$4T_E+2T_H+2T_M$
本文方案	$2T_E+1T_H+1T_M$	$2T_E+1T_H+1T_M$	$4T_E+2T_H+2T_M$

为了展示本方案的实际计算开销和相对应的时间开销曲线图，本文对方案在集成开发环境 Visual 2012 中用 C++进行了代码实现，在代码实现过程中用到密码学库 Crypto++。实现环境主要参数如表 2 所示。

表 2 实验环境主要参数

Table 2 Main parameters of the experimental environment

项目	参数
操作系统版本	Windows 7 旗舰版 Service Pack 1
系统类型	64 位操作系统
处理器	Intel(R) Core™ i5-4590S CPU @ 3.00 GHz
安装内存	4.00 GB

当签密者和指定验证者的私钥确定（本实验中 $|x_a|=|x_b|=512$），当消息长度不同时，签密与解签密过程运行时间曲线图如图 3 所示。

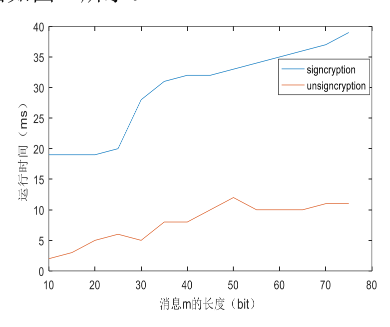


图 3 签密与解签密过程运行时间曲线图

Fig. 3 The running time of signcryption and unsigncryption

通过理论和实现分析，并得出结论：本方案高效且具有一定的实际应用价值。

5 结束语

本文对 Sujata 方案进行授权攻击，并提出了一个基于离散对数问题的强指定验证者的签密方案。本方案不需要安全的信道就可实现签密者和指定验证者之间的秘密传输[15]。本方案被证明在适应性选择明文攻击下是安全的。此外，本方案满足不可授权这一安全要求，并且可以防止签密传输过程中密文被窜改的情况[16]，因此本文的方案有很多实际的应用，比如在区块链资产证明[17, 18]、电子投票等领域。

参考文献：

[1] Zheng Yuliang. Digital signcryption or how to achieve cost (signature&encryption) <<cost (signature) +cost (encryption) [C]// . Advancesin Cryptology. Berlin: Springer, 1997: 165-179.

[2] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications [C]// Advances in Cryptology. Berlin: Springer, 1996: 143-154.

[3] Saeedina S, Kremer S, Markowitch O. An efficient strong designated verifier signature scheme [C]//Proc of International Conference on Information Security and Cryptology. Berlin: Springer, 2004: 40-54.

[4] Lipmaa H, Wang Guilin, Bao Feng. Designated verifier signature schemes: attacks, newsecurity notions and a new construction [C]//Proc of the 32nd International Colloquium-ICALP2005. BerlinHeidelberg: Springer, 2005: 459-471.

[5] Sujata Mohanty, Banshidhar Majhi. A Strong Designated Verifiable DL Based Signcryption Scheme [J]. Journal of Information Processing Systems, 2012, 8 (4): 567-574.

[6] Tan C H. Analysis of improved signcryption scheme withkey privacy [J]. Information Processing Letters, 2006, 99(4): 135-138.

[7] Huang Qiong, Willy S, Wong D S. Non-delegatable Identity-based Designated Verifier Signature [R]. Cryptology ePrintArchive: Report 2009.

[8] Yang Xiaoyuan, Yu Qingfei. ECC-based new designated verifier signature scheme [J]. Journal of PLA University of science and Technology, 2007, 35(8): 1432-1436.

[9] Lee J, Chang J. Comment on Saeednia *et al.* 's strong designated verifier signature scheme [J]. Computer Standards&Interfaces, 2009, 8(31): 258-260.

[10] Schnorr C P. Efficient signature generation for smart cards [J]. Journal of Cryptology, 1991, 4(3): 239-252.

[11] Wang Guilin, Bao Feng, Ma Changshe, *et al.* Efficient authenticated encrptionschemes with public verifiability[C]//Proc of the 60th IEEE Vehicular Technology Conference on Wireless Technologies for Global Security.Washington DC: IEEE Computer Society, 2004: 3258-3261.

[12] Petersen H, Michels M. Cryptanalysis and improvement of signcryption schemes [J]. IEEE Computers and Digital Communications, 1998, 8(2): 149-151.

[13] Yang Guomin, Wong D S, Deng Xiaotie. Analysis and improvementof Petersen-Michels signcryption scheme with key privacy [C]//Proc of Information Security Conference. Singapore: Springer, 2005: 218-232.

[14] Huang Qiong, Yang Guomin, Wong D S, *et al.* Identity-based strong designated verifier signature revisited [J]. Journal of Systems and Software, 2011, 84(1): 120–129.

[15] Yang Bo, Sun Ying, Yu Yong, *et al.* A Strong designated verifier signature scheme with secure disavowability [C]//Proc of International Conference on Intelligent Networking &Collaborative Systems. Bucharest. Romania: IEEE SMC, 2012: 286-291.

[16] Yang Bo, Yu Yong, Sun Ying. A novel construction of SDVS with securedisavowability [J]. Cluster Computing, 2013, 16(4): 807-815.

[17] Koochak S M, Ahmadian-Attari M, Aref M R. Provably secure strong designated verifier signature scheme based on coding theory [J]. International Journal of Communication Systems, 2016, 30 (7): 1099-1131.

[18] Wang Huaqun, He Debiao, Ji Yimu. Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography [J]. Future Generation Computer Systems, 2017, 84(1): 135-137.